09/936131
518 Rec'd PCT/PTO 06 SEP 2001

EXPRESS MAIL NO. EL652176548US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Boris BALECHEFF, et al.	Re: Claim to Priority
U.S. Appln. No.: not yet assigned	Group: not yet assigned
U.S. Filing Date: concurrently herewith	Examiner: not yet assigned
International Application No: PCT/GB00/00752	
International Filing Date: 3 March 2000	Our Ref.: B-4295PCT 619055-2
For: "SMARTCARD USER INTERFACE FOR TRUSTED COMPUTING PLATFORM	Date: September 4, 2001

35 U.S.C. 119 CLAIM TO PRIORITY

Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Attn: United States Designated/Elected Office (DO/EO/US)

Sir:

Prior PCT International Application No. PCT/GB00/00752, designating the U.S., claims foreign priority as follows:

COUNTRY	FILING DATE	SERIAL NUMBER
Great Britain	5 March 1999	9905056.9
Great Britain	15 December 1999	9929697.2

The certified copies have been filed in prior PCT International Patent Application No. PCT/GB00/00752.

Applicants hereby confirm that this claim for priority applies to the above-identified U.S. International stage application.

Respectfully submitted,

Richard P. Berg
Reg. No. 28,145
Attorney for Applicant
LADAS & PARRY
5670 Wilshire Boulevard #2100
Los Angeles, California 90036
(323) 934-2300

PCT/GB 0 0 / 0 0 7 5 2

The Patent Office

03 MARCH 2000

INVESTOR IN PEOPLE

EJU

09/936131

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP9 1RH

REC'D 10 APR 2000
WIPO PCT

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed

Dated 6/5/99

Patents Form 1/77

Patents Act 1977
(Rule 16)

The Patent Office

05MAR99 E430380-1 D01468
700 0.00 - 9905056.9

THE PATENT OFFICE
A
-5 MAR 1999
RECEIVED BY FAX

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office

Cardiff Road
Newport
Gwent NP9 1RH

1. Your reference — 30990059 GB

2. Patent application number *(The Patent Office will fill in this part)* — **9905056.9** — 5 MAR 1999

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

HEWLETT-PACKARD COMPANY
3000 Hanover Street
Palo Alto
California 94304
United States of America

Patents ADP number *(if you know it)* 4965886002

If the applicant is a corporate body, give the country/state of its incorporation — Delaware, USA

4. Title of the invention

Computing apparatus & methods of operating computer apparatus

5. Name of your agent *(if you have one)* — Matthew John Mitchell Lawman

"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

Hewlett-Packard Limited
Intellectual Property Section
Filton Road
Stoke Gifford
Bristol BS12 6QZ

Patents ADP number *(if you know it)* 1937005

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number

Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing *(day / month / year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:*

a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d))

YES

Pate[illegible]s Form 1/77

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form	0
Description	16 /
Claim(s)	4 /
Abstract	0
Drawing(s)	7 /

10. If you are also filing any of the following, state how many against each item.

Priority documents	
Translations of priority documents	
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	
Request for preliminary examination and search *(Patents Form 9/77)*	1 /
Request for substantive examination *(Patents Form 10/77)*	/
Any other documents *(please specify)*	1 / (Fee Sheet)

11. I/We request the grant of a patent on the basis of this application.

Signature [signature] Date 5 March 1999

Matthew John Mitchell Lawman

12. Name and daytime telephone number of person to contact in the United Kingdom

0117-312-9946 - M J M Lawman or
0117-312-8026 - J C Smith

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.

b) Write your answers in capital letters using black ink or you may type them.

c) If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.

d) If you have answered 'Yes' Patents Form 7/77 will need to be filed.

e) Once you have filled in the form you must remember to sign and date it.

f) For details of the fee and ways to pay please contact the Patent Office.

DUPLICATE

COMPUTING APPARATUS AND METHODS OF OPERATING COMPUTING APPARATUS

(HP Ref: 3099059)

Technical Field

This invention relates to computing apparatus and particularly, but not exclusively, to computing apparatus and methods of operating computing apparatus in a secure environment using security tokens.

Background Art

Security tokens, for example smart cards or cryptographic co-processors, have recently been proposed for various security functions including accessing computer platforms (or 'host platforms') and electronic commerce. For instance, a smart card storing confidential information accessible only to a related user can be used by the user to log on to a computer, to sign a document, or to provide credentials needed for electronic commerce.

In some cases, it is expected that more than one security token for plural different applications may need to be used in a single communication session, which starts as the user logs on to a host platform and finishes as the user logs off.

One possible model works as follows. A user has a number of tokens and, in each session, they use one of these tokens (for example, a logon token) for authentication to a host platform in the logon process only. During the same session, the user separately uses other tokens (for example, auxiliary tokens) for other security functions, such as electronic payment or cryptography.

Disclosure of the Invention

In arriving at the present invention, the present inventors have appreciated the following three potential problems with this model:

Problem A - there is an inherent danger of a user walking away after logging on to the host platform, thus allowing an impostor to use the platform.

Problem B - a fake host platform may be able to steal sensitive information from the user.

Problem C - there are some auxiliary tokens whose owner's identities are not traceable to the owner of the logon token. In other words, an impostor, who does not own the logon token, may be able to use his own auxiliary tokens to impersonate the logon token's owner.

In addressing one or more of the above problems, the present inventors propose a new arrangement to reduce security risk and to establish a more trusted relationship

between a host platform and one or more security tokens. Typically, the arrangement implements a security control policy that is more refined than the policy in the prior art model, including periodic or repeated authentication. Preferred embodiments of the invention implement mutual authentication and privilege restriction. In particular, p[redacted]d embodiments utilise a novel method of binding the identity of a logon, or primary, s[redacted]ty token with one or more auxiliary tokens. Of utmost importance is that the invention meets the important criteria of being easy to use at relatively cheap to implement compared with prior art solutions.

In accordance with a first aspect, the present invention provides computing apparatus comprising:

memory means storing the instructions of a secure process and an authentication process;

processing means arranged to control the operation of the computing apparatus including by executing the secure process and the authentication process as required;

user interface means arranged to receive user input and return to the user information generated by the processing means in response to the user input; and

interface means for receiving a removable primary token and communicating with the token, the token comprising a body supporting:

a token interface for communicating with the interface means;

a token processor; and

token memory storing token data including information for identifying the token,

wherein the processing means is arranged to receive the identity information from the primary token, authenticate the token using the authentication process and, if the token is successfully authenticated, permit a user to interact with the secure process via the user interface means,

and wherein the processing means is arranged to repeatedly authenticate the primary token and cause the computing platform to suspend interaction between the secure process and the user if authentication is not possible as a result of the removal of the primary token.

In accordance with a second aspect, the present invention provides a method of controlling computing apparatus to authenticate a user, comprising the steps:

the computing apparatus receiving a primary token of the user, the primary token containing information suitable for authenticating the primary token;

if the token is authentic, permitting the user to interact with one or more secure applications that may be executed by the computing platform;

at intervals, re-authenticating the primary token; and

if it is not possible to re-authenticate the primary token, suspending the interaction between the computing apparatus and the user.

Other aspects of the invention will become apparent from the accompanying description, claims and drawings.

Brief Description of the Drawings – **to be updated**

Preferred embodiments of the present invention will now be described, by way of example only, with reference to the accompanying drawings, of which:

Figure 1 is a diagram which illustrates a system capable of implementing embodiments of the present invention;

Figure 2 is a diagram which illustrates a motherboard including a trusted device arranged to communicate with a number of smart cards via a single smart card reader;

Figure 3, is a diagram that illustrates the trusted device in more detail;

Figure 4 is a diagram that illustrates the operational parts of a logon smart card according to the present invention;

Figure 5 is a flow diagram which illustrates the process of mutually authenticating a logon smart card and a host platform;

Figure 6 is a flow diagram which illustrates one general example of introducing an auxiliary smart card to a host platform using by a logon smart card;

Figure 7 is a flow diagram which illustrates one example of the operation between an introduced cash card and the host platform;

Figure 8 is a flow diagram which illustrates one example of a single session temporary delegation mode; and

Figure 9 is a flow diagram which illustrates one example of a multiple session temporary delegation mode.

Best Mode For Carrying Out the Invention, & Industrial Applicability

While the ideas of the invention are general, for ease of discussion, we will focus on preferred embodiments, wherein smart cards are the security tokens, which interact with a trusted computing platform, or simply "platform". In particular, a user has one logon smart card and a number of auxiliary smart cards, and needs to interact with the platform, which has only a single smart card reader. It is assumed in the present embodiment that there is no way for more than one smart card to be read by the smart card reader at the same time.

In order to address Problem A, as highlighted in the "Description of Prior Art", the present embodiments implement a coherent security control policy using a logon smart card operating with the platform. Specifically, to limit the potential for an impostor getting access to the trusted platform without the legitimate user's knowledge, the logon smart card must be present throughout the session, rather than just to initiate the session. By analogy, the logon smart card is used more like a car key than a door key.

In effect, a user is held responsible for their actions. Since the smart card has to be present during the execution of a command, this effectively and unambiguously holds the owner of the smart card responsible for the action. As will be described below, the authentication is done automatically by the platform and does not generally require actions from the user. This amounts to a saving of time for the user and is, thus, a very attractive feature.

A major strength of the proposed scheme lies in its intuitive appeal. People are familiar with the importance of protecting their keys and accept full responsibility for respective misuse of the keys. The present scheme, which greatly enhances security, is simple to implement. As an added security feature, it is preferable that the logon smart card is also password protected, requiring a user to enter a password when the card is first inserted into the smart card reader. Password techniques are well-known and will not be described herein, so as not to obscure the Invention.

Generally, to check the presence of the logon smart card, the platform needs repeatedly to authenticate the logon card. The actual frequency of the authentication can be configured by either a system administrator or the user. In practice, one would set the frequency high enough that the user, or an unauthorised user, would be unable to subvert the platform and carry out an unauthorised transaction between authentications. For example, authentication may occur every few seconds.

A further security feature that can be implemented in the security policy is a time-limit for each authenticated session using an auxiliary smart card. The user interface may also be locked unless a new round of authentication is performed within the pre-set time-limit. Further, preferably, time-stamping, or the use of nonces, is used to prevent "replay attacks" during authentication.

To address the fake host platform problem, Problem B above, the preferred embodiments use the concept of a trusted device built into the platform, which allows a user to verify the integrity of the platform. The concept of such a trusted device is the subject of the applicant's co-pending European patent application entitled "Trusted Computing Platform" filed on 15 February 1999, the entire contents of which are hereby incorporated herein by reference.

To address Problem C, as highlighted in the "Description of Prior Art", where an auxiliary smart card may not be traceable to the owner of the logon smart card, the present embodiments introduce the concept of a user profile that binds a user to a number of auxiliary smart cards. This makes the implementation of a coherent, comprehensive and flexible security control policy extremely simple, inexpensive and transparent to the user.

Generally, in the preferred embodiments, it is always assumed that logging on is done by a logon smart card, and at some point of the session, the user (or the application running under the session) needs to use one or more auxiliary smart cards, so that removal of the logon card becomes necessary. To maintain the security policy of repeated authentication, there needs to be a security chain for the platform between trusting the logon smart card and trusting other auxiliary smart cards. This chain is built by letting the logon smart card 'introduce' the auxiliary cards to the platform, for example by using 'user profiles'.

For the sake of simplicity of description, only two types of auxiliary smart cards are considered in any detail herein:

"Cash cards", which are smart cards having cash values (or credits) that are transferable; and

"Crypto cards", which are smart cards whose privileges (such as encryption or signature supported by a private key) are not transferable.

A trusted platform 10 incorporating a smart card reader 12 is illustrated in the diagram in Figure 1. The platform 10 includes the standard features of a keyboard 14, mouse 16 and visual display unit (VDU) 18, which provide the physical 'user interface' of the platform. Along side the smart card reader 12, there are illustrated a logon smart card 19 and plural auxiliary smart cards 20.

Conveniently, the present invention uses the platform that is described in detail in the present applicant's co-pending patent application referred to above. While this platform is ideal for the purposes of the present embodiment, and allows a user to verify the integrity of the platform, use of the platform is by no means essential to the present invention. In particular, the present invention does not necessarily require a user to verify the integrity of the platform, which might be acceptable, for example, if the platform is a private platform in a users own home. The main advantage of using a platform having a trusted device is realised in an environment where many users potentially have access to the platform, thereby providing reasonable opportunity for the platform to be subverted in some way. The main features of a platform including a trusted device will now be reproduced herein purely for the reader's convenience.

As illustrated in Figure 2, the motherboard 20 of the trusted computing platform 10 (as described in the applicant's co-pending application) includes (among other standard

components) a main processor 21, main memory 22, a trusted device 24, a data bus 26 and respective control lines 27 and address lines 28, BIOS memory 29 containing the BIOS program for the platform 10 and an Input/Output (IO) device 23, which controls interaction between the components of the motherboard and the smart card reader 12, the keyboard 14, the mouse 16 and the VDU 18. The main memory 22 is typically random access memory (RAM). In operation, the platform 10 loads the operating system, for example Windows NT™, into RAM from hard disk (not shown). Additionally, in operation, the platform 10 loads the processes or applications that may be executed by the platform 10 into RAM from hard disk (not shown). In the present case, the key applications are an authentication application and a secure application, the operations of which will be described below.

Typically, for a conventional IBM-compatible platform (i.e. a "PC"), the BIOS program is located in a special reserved memory area, the upper 64K of the first megabyte do the system memory (addresses FØØØh to FFFFh), and the main processor is arranged to look at this memory location first, in accordance with an industry wide BIOS standard.

A significant difference between the present trusted platform 10 and a conventional platform is that, after reset, the main processor 21 is initially controlled by the trusted device 24, which then hands control over to the platform-specific BIOS program, which in turn initialises all input/output devices as normal. After the BIOS program has executed, control is handed over as normal by the BIOS program to the operating system.

The trusted device 24 comprises a number of blocks, as illustrated in Figure 3. After system reset, the trusted device 24 performs a secure boot process to ensure that the operating system of the platform 10 (including the system clock and the display on the monitor) is running properly and in a secure manner. During the secure boot process, the trusted device 24 acquires an integrity metric of the computing platform 10. The trusted device 24 can also perform secure data transfer and, for example, authentication between it and a smart card via encryption/decryption and signature/verification. The trusted device 24 can also securely enforce various security control policies to be discussed below including frequent authentication and the locking of user interface.

Specifically, the trusted device 24 comprises: a controller 30 programmed to control the overall operation of the trusted device 24, and interact with the other functions on the trusted device 24 and with the other devices on the motherboard 10; a measurement function 31 for acquiring the integrity metric from the platform 10; a cryptographic function 32 for signing, encrypting or decrypting specified data; an authentication function 33 for authenticating a logon smart card 19; and interface circuitry 34 having appropriate ports (36, 37 & 38) for connecting the trusted device 24 respectively to the data bus 26, control lines 27 and address lines 28 of the motherboard 10. Each of the blocks in the trusted device 24 has

access (typically via the controller 20) to appropriate volatile memory areas 37 and/or non-volatile memory areas 38 of the trusted device 24. Additionally, the trusted device 24 is designed, in a known manner, to be tamper resistant.

For reasons of performance, the trusted device 24 may be implemented as an application specific integrated circuit (ASIC). However, for flexibility, the trusted device 24 is preferably an appropriately programmed micro-controller. Both ASICs and micro-controllers are well known in the art of microelectronics and will not be considered herein in any further detail.

One item of data stored in the non-volatile memory of the trusted device 24 is a certificate 350. The certificate 350 contains at least a public key 351 of the trusted device 24 and an authenticated value 352 of the platform integrity metric measured by a trusted party (TP). The certificate 350 is signed by the TP using the TP's private key prior to it being stored in the trusted device 24. In later communications sessions, a user of the platform 10 can verify the integrity of the platform 10 by comparing an acquired integrity metric with the authentic integrity metric 352. If there is a match, the user can be confident that the platform 10 has not been subverted. Knowledge of the TP's generally-available public key enables simple verification of the certificate 350. The non-volatile memory 35 also contains an identity (ID) label 353. The ID label 353 is a conventional ID label, for example a serial number, that is unique within some context. The ID label 353 is generally used for indexing and labelling of data relevant to the trusted device 24, but is insufficient in itself to prove the identity of the platform 10 under trusted conditions.

The trusted device 24 is equipped with at least one method of reliably measuring or acquiring the integrity metric of the computing platform 10 with which it is associated. In the present embodiment, the integrity metric is acquired by the measurement function 31 by generating a digest of the BIOS instructions in the BIOS memory. Such an acquired integrity metric, if verified as described above, gives a potential user of the platform 10 a high level of confidence that the platform 10 has not been subverted at a hardware, or BIOS program, level. Other known processes, for example virus checkers, will typically be in place to check that the operating system and application program code has not been subverted.

The measurement function 31 has access to: non-volatile memory 35 for storing a hash program 354 and a private key 355 of the trusted device 24: and volatile memory 42 for storing the public keys and associated ID labels 360a-360n of one or more authentic logon smart card 19s that can be used to gain access to the platform 10, and an acquired integrity metric in the form of a digest 361.

A processing part 40 of a logon smart card 19 is illustrated in Figure 4. As shown, the logon smart card 19 40 has the standard features of a processor 41, memory 42 and

interface contacts 43. The processor 41 is programmed for simple challenge/response operations involving authentication of the logon smart card 19 and verification of the platform 10, as will be described below. The memory 42 contains its private key 420, its public key 428, a user profile 421, the public key 422 of the TP and an identity 427. The user profile 421 lists the allowable auxiliary smart cards 20 AC1-ACn usable by the user, and the individual security policy 424 for the user. For each auxiliary smart card 20, the user profile includes respective identification information 423, the trust structure 425 between the smart cards (if one exists) and, optionally, the type or make 426 of the smart card.

In the user profile 421, each auxiliary smart card 20 entry AC1-ACn includes associated identification information 423, which varies in dependence upon the type of card. For example, identification information for a cash card typically includes a simple serial number, whereas, for a crypto card, the identification information typically comprises the public key (or certificate) of the crypto card (the private key being stored secretly on the crypto card itself).

The 'security policy' 424 dictates the permissions that the user has on the platform 10 while using an auxillary smart card 20. For example, the user interface may be locked or unlocked while an auxiliary smart card 20 is in use, depending on the function of the auxiliary smart card 20. Additionally, or alternatively, certain files or executable programs on the platform 10 may be made accessible or not, depending on how trusted a particular auxiliary smart card 20 is. Further, the security policy 424 may specify a particular mode of operation for the auxiliary smart card 20, such as 'credit receipt' or 'temporary delegation', as will be described below.

A 'trust structure' 425 defines whether an auxiliary smart card 20 can itself 'introduce' further auxiliary smart cards 20 into the system without first re-using the logon smart card 19. In the embodiments described in detail herein, the only defined trust structure is between the logon smart card 19 and the auxiliary smart cards 20 that can be introduced to the platform 10 by the logon smart card 19. Introduction may be 'single session' or 'multi-session', as will be described below. However, there is no reason why certain auxiliary smart cards 20 could not in practice introduce further auxiliary smart cards 20. This would require an auxiliary smart card 20 to have an equivalent of a user profile listing the or each auxiliary smart card that it is able to introduce.

A preferred process for authentication between a logon smart card 19 and a platform 10 will now be described with reference to the flow diagram in Figure 5. As will be described, the process conveniently implements a challenge/response routine. There exist many available challenge/response mechanisms. The implementation of an authentication protocol used in the present embodiment is mutual (or 3-step) authentication, as described in

ISO/IEC 9798-3 [1]. Of course, there is no reason why other authentication procedures cannot be used, for example 2-step or 4-step, as also described in [1].

Initially, the user inserts their logon smart card 19 into the smart card reader 12 of the platform 10 in step 500. Beforehand, the platform 10 will typically be operating under the control of its standard operating system and executing the authentication process, which waits for a user to insert their logon smart card 19. Apart from the smart card reader 12 being active in this way, the platform 10 is typically rendered inaccessible to users by 'locking' the user interface (i.e. the screen, keyboard and mouse).

When the logon smart card 19 is inserted into the smart card reader 12, the trusted device 24 is triggered to attempt mutual authentication in step by generating and transmitting a nonce A to the logon smart card 19 in step 505. A nonce, such as a random number, is used to protect the originator from deception caused by replay of old but genuine responses (called a 'replay attack') by untrustworthy third parties.

In response, in step 510, the logon smart card 19 generates and returns a response comprising the concatenation of: the plain text of the nonce A, a new nonce B generated by the logon smart card 19, the ID 353 of the trusted device 24 and some redundancy; the signature of the plain text, generated by signing the plain text with the private key of the logon smart card 19; and a certificate containing the ID and the public key of the logon smart card 19.

The trusted device 24 authenticates the response by using the public key in the certificate to verify the signature of the plain text in step 515. If the response is not authentic, the process ends in step 520. If the response is authentic, in step 525 the trusted device 24 generates and sends a further response including the concatenation of: the plain text of the nonce A, the nonce B, the ID 427 of the logon smart card 19 and the acquired integrity metric; the signature of the plain text, generated by signing the plain text using the private key of the trusted device 24; and the certificate comprising the public key of the trusted device 24 and the authentic integrity metric, both signed by the private key of the TP.

The logon smart card 19 authenticates this response by using the public key of the TP and comparing the acquired integrity metric with the authentic integrity metric, where a match indicates successful verification, in step 530. If the further response is not authentic, the process ends in step 535.

If the procedure is successful, both the trusted device 24 has authenticated the logon smart card 19 and the logon smart card 19 has verified the integrity of the trusted platform 10 and, in step 540, the authentication process executes the secure process for the user. Then, the authentication process sets an interval timer in step 545. Thereafter, using appropriate operating system interrupt routines, the authentication process services the interval timer

periodically to detect when the timer meets or exceeds a pre-determined timeout period in step 550.

Clearly, the authentication process and the interval timer run in parallel with the secure process.

When the timeout period is met or exceeded, the authentication process triggers the trusted device 24 to re-authenticate the logon smart card 19, by transmitting a challenge for the logon smart to identify itself in step 560. The logon smart card 19 returns a certificate including its ID 427 and its public key 428 step 565. In step 570, if there is no response (for example, as a result of the logon smart card 19 having been removed) or the certificate is no longer valid for some reason (for example, the logon smart card has been replaced with a different smart card), the session is terminated by the trusted device 24 in step 575. Otherwise, in step 570, the process from step 545 repeats by resetting the interval timer.

A preferred, general process for introducing an auxiliary smart card 20 into a platform 10 will now be described with reference to the flow diagram in Figure 6.

When the secure process running on the platform 10 reaches a point where the logon smart card 19 needs to be replaced by an auxiliary smart card 20, for example at the time a cash card is needed to credit the platform 10 with funds for a remote transaction, in step 605 the secure process retrieves the user profile from the trusted device 24 and stores it in its volatile memory 35. The trusted device 24 then extracts the details of the auxiliary smart cards (AC) 20 from the user profile and returns the details to the secure process in step 610. In step 615, the secure process displays an option list of auxiliary smart cards 20 and asks the user to select one. The secure process receives the users selection in step 620 and displays a message asking the user to replace the logon smart card 19 with the (or one of the) selected auxiliary smart card(s) 20 in step 625. As soon as the user ejects the logon smart card 19, the trusted device locks the user interface in step 630 and, in step 635, the secure process initialises the authentication process interval timer with a new timeout period, which determines the allowable duration of the auxiliary smart card session.

[In parallel with the operation of the secure process, which has been described with reference to Figure 5), if the timeout period expires before the logon smart card 19 has been reinstated, the authentication process suspends the session (i.e. the secure process) and provides the user with an appropriate message. The authentication process has the authority to suspend the secure process, since it executed the secure process in the first instance. Clearly, the new timeout period needs to be sufficient for the required purposes, and may be configurable by a system administrator for this reason.]

When the user inserts the selected auxiliary smart card 20, the trusted device 24 is triggered to send the auxiliary smart card 20 a challenge to identify itself in step 640. The

auxiliary smart card 20 responds by returning its identity information to the trusted device 24 in step 645. The trusted device 24 then verifies the identity information by comparing it with the stored user profile information in step 650.

If the trusted device 24 is unable to verify the auxiliary smart card 20 for any reason, in step 655 the session ends and the secure process displays an appropriate message for the user. Otherwise, in steps 660 and 665, the secure process interacts with the auxiliary smart card 20 as required.

When the interaction is complete, in step 670, the secure process displays a prompt to the user to replace the auxiliary smart card 20 with the logon smart card 19. When the user ejects the auxiliary smart card 20 form the smart card reader 12 and inserts the logon smart card 19, the trusted device 24 is triggered to authenticate the logon smart card 19, by executing from step 560 in Figure 5, as described above, resulting in the session ending in step 575 or continuing in step 545.

Additionally, or alternatively, in some embodiments it may be required that the user profile is encrypted and signed to protect privacy and integrity. If so, a secure data transfer protocol may be needed between the trusted device 24 and the logon smart card 19. There exist many available mechanisms for transferring secure credentials between two entities. A possible implementation, which may be used in the present embodiment, is secure key transport mechanisms from ISO/IEC DIS 11770-3 [2].

Clearly, the operation of the process that has just been described for introducing an auxiliary smart card 20 may vary in dependence upon the type of the auxiliary smart card 20; for example, whether it is a cash card or a crypto card. Variations in process for different types of auxiliary smart card 20 will now be described.

CREDIT RECEIPT MODE

A credit receipt mode allows a user to remove the logon smart card 19 for a very brief period of time (say 2 minutes, which is configurable by a system administrator or a user) from the smart card reader 12 to allow credits (or cash values) from a cash card to be transferred to the trusted device 24 of the platform 10 without undue security risk.

Figure 7 illustrates the process for enacting credit receipt mode. The steps that correspond to those illustrated in Figure 6 will not be specifically described again.

It is assumed that a user profile that lists auxiliary smart cards 20 including cash cards is stored in the logon smart card 19. As before, when a user invokes an application that requires cash values, the secure process displays a request for the user to choose a cash card from those listed in the user profile.

The first difference between the credit receipt mode process and the process in Figure 6 is that in step 721 the secure process displays a further request for the user to enter the amount of the credit transfer. The secure process receives the entered amount in step 722 and forwards a respective value to the trusted device 24 in step 723. The trusted device 24 transfers the credits from the cash card to the trusted device 24 in steps 760 and 765, after the cash card has been inserted and authenticated.

As an alternative or additional feature, depending on the security policy, unauthorised cash cards may also be used; for example, there may be an option "Others" in the list of authorised cash cards. Clearly, the risks associated with receiving credits from any auxiliary smart card 20 are relatively low.

Typically, only a relatively short time is required to enact the whole process of transferring the credits. The length of the timeout period is determined by the security policy in the user profile. If the timeout is exceeded, the transfer process is aborted and the user interface is temporarily locked. On the other hand, if the user reinserts the logon smart card 19 within the specified time-limit, a new round of authentication is performed between the smart card and the platform 10. Upon successful verification, the user interface will be unlocked and the original session, i.e. before the credit transfer mode, resumes, but with the cash value now stored in the trusted device 24. The cash value may be used for, for example, electronic commerce.

Since the user interface is essentially locked during the credit transfer mode, and is re-activated only after the re-insertion of the logon smart card 19, the host platform 10 does not suffer any serious security risk in the credit receipt mode. Further, since the user has to authenticate which cash card to use, using the logon smart card 19, abuse of cash cards by illegal users is also minimised.

TEMPORARY DELEGATION MODES

It will be appreciated that for a crypto card to function (say for encryption, decryption, signature and verification), it potentially needs to be inserted in the place of a logon card for a substantial amount of time, unlike for cash cards. To address the need for potentially greater periods of time to use a crypto card, the present embodiment includes what is referred to as a temporary delegation mode, which allows a user to use crypto cards in place of the logon card for an undefined time, subject to possible respective security policy limitations. Temporary delegation modes will now be described with reference to the flow diagram in Figure 8. The steps that correspond to those illustrated in Figure 6 will not be specifically described again.

To invoke a temporary delegation mode, a user (or the secure process) selects a temporary delegation mode in step 800 while the logon smart card 19 is being used. In response, the host platform 10 takes the steps to receive and authenticate the auxiliary smart card 20, which in this example is a crypto card.

When provided with a list of allowable crypto cards, the user specifies the authorised crypto card. Depending on the security policy, unregistered crypto cards may or may not be used. Again, if the user profile is encrypted, a secure data transfer protocol (again, see [2]) may be employed.

After the logon smart card 19 is removed, the user interface is locked and a the secure process displays a message requesting a new smart card.

Upon insertion and authentication of the specified crypto card, the secure process activates user privileges in step 833 consistent with the security policy of the crypto card. For example, the user may need to use the user interface for entry of certain information related to the crypto card operation, but should not be able to execute any other process or perform any other operation.

When the crypto card is removed from the smart card reader 12, the user interface is locked again, until the logon smart card 19 is inserted and authenticated.

The example of the temporary delegation mode described above allows a single auxiliary smart card 20 to be used in a 'single session' in place of the logon smart card 19 for an undefined period of time.

An alternative, or additional, temporary delegation mode permits multiple auxiliary smart cards 20 to be used in turn, in place of the logon smart card 19, without the need to re-insert the logon smart card 19. An example of such a 'multi-session' temporary delegation mode will now be described with reference to Figure 9. As before, the steps that correspond to those illustrated in Figure 6 will not be specifically described again.

In a multi-session, multiple auxiliary smart cards 20 can be freely used in place of the logon smart card 19, thus allowing maximal convenience of use.

To invoke a multi-session temporary delegation mode, a user (or the secure process) selects a multi-session temporary delegation mode in step 900 while the logon smart card 19 is being used.

A significant difference between a multi-session temporary delegation mode and the single session temporary delegation mode is that, when provided with the list of available authorised auxiliary smart cards 20 in step 915, the user can select multiple authorised auxiliary smart cards 20 in step 920. The selected auxiliary smart cards 20 may be of different kinds depending on the user's requirements.

The host platform 10 takes the steps to receive and authenticate any one of the selected auxiliary smart cards 20.

As soon as the logon smart card 19 is ejected the user interface is locked, the secure process activates user privileges consistent with the operation of that auxiliary smart card 20 in step 933. When the auxiliary smart card 20 is eventually ejected, the process loops to step 925, a message is generated to replace the card and the user interface is locked again in step 930. When the next auxiliary smart card 20 is inserted, the secure process activates user privileges consistent with the operation of that auxiliary smart card 20 in step 933 again.

This procedure may be repeated for any of the selected auxiliary smart cards 20 until the session ends or the logon smart card is re-inserted in step 975. In other words, the user can use any combination of the selected auxiliary smart cards 20 without the need of the insertion of the logon smart card 19 during the whole multi-session. Clearly, such a permissive multi-session is very convenient for the user, although the benefits need to be weighed against the risks of such freedom.

Note that a security control policy described in the user profile may give constraints on the number, types and makes of smart cards allowed in a multi-session as well as any time-limits. Typically, different auxiliary smart cards 20 give the user different sets of privileges. For instance, some sensitive files may be locked whenever the auxiliary smart card 20 currently being used is regarded to be not trustworthy enough. Indeed, any truly sensitive application may require the insertion of the logon smart card 19 again for authentication.

Since it is not easy to estimate how long a temporary delegation mode will last, in theory, it might be acceptable to have no timeout period as such, as in the examples above. However, there are risks associated with such a policy, for example a user may leave the platform 10 during a temporary delegation mode session. Therefore, it is preferable to have an overall timeout period, fixed for the temporary delegation mode session, which overrides both the normal re-authentication timeout period of the authentication process and the individual timeout periods associated each auxiliary smart card 20. Additionally, it might also be possible to have individual timeout periods for certain auxiliary smart cards 20. As usual, the specification of the timeout period(s) will be determined by the security policies for the auxiliary smart cards 20. In practice, the timeout period for a temporary delegation mode is implemented by the secure process overriding the authentication process. Exemplary fixed session timeout periods for temporary delegation modes are 30 minutes, 1 hour or 2 hours. The period(s) can be set or modified by the user or a system administrator, and may depend on the trustworthiness of the platform 10.

Re-insertion of the original logon card will typically be needed for extending the temporary delegation mode session, and, generally, the secure process issues a warning message to the user prior to expiration. This is analogous to request for insertion of coins in a phone booth during phone calls. Upon expiration, the user interface will be locked and can be unlocked only by the logon card. If a user attempts to use a time-consuming application in a temporary delegation mode, the secure process may request the insertion of a logon smart card 19 beforehand to avoid locking the user interface in the middle of an application.

There are a variety of possible, different temporary delegation modes that generally specify the class of auxiliary smart cards 20 and applications allowed during the temporary delegation mode. For instance, in some modes, perhaps only a single type of auxiliary smart card 20 (possibly with traceable ID) is allowed. In other modes, only a small class of auxiliary smart cards 20 is allowed. In yet other modes, a large class of auxiliary smart cards 20 is allowed.

The exact set of privileges that can be delegated is a function of the system security policy, a choice by the user (in set-up and/or during the session itself), and the type and make of the auxiliary card being used. Some privileges may be revoked during a temporary delegation mode. For instance, some files (currently on screen or otherwise) may become locked once the temporary delegation mode is employed. High security applications might request the re-insertion of the original logon card. In an extreme case, all privileges except for the specific application may be temporarily suspended during the temporary delegation mode.

As an alternative, or in addition, to the embodiments described above, the logon smart card 19 may be programmed to categorise different platform 10s. For example, platform 10s may be categorised as "fairly trustworthy", "very trustworthy", or "extremely trustworthy", depending on the type of the platform 10. In this case, the platform 10 type will be revealed by the identity information received by the logon smart card 19 from the platform 10. The logon smart card 19 is programmed to compare the identity information with pre-determined, stored information, where a particular match indicates the category of the platform 10. Conveniently, the stored category information forms part of the user profile.

The security policy that the logon smart card 19 adopts with a particular platform 10 then depends on the category of the platform 10. In one example, the logon smart card 19 may transmit different user profile information to the platform 10 depending on the platform 10's category. For example, with a "fairly trustworthy" platform 10, the smart card might only pass information relating to crypto cards to the platform 10, to restrict the user to only being able to send and receive encrypted emails, or surf the Internet. Additionally, for "fairly trustworthy" platform 10s, the user profile information may limit to 'single-session' temporary

delegation modes. In contrast, a "very trustworthy" platform 10 may receive user profile information that permits multi-session temporary delegation modes and even cash card transactions. Finally, an "extremely trusted" platform 10 would receive user profile information to permit all possible actions including multi-session and cash card transactions but also other administrative functions.

An example of an administrative function, requiring an "extremely trusted" platform 10, is the ability to create or modify the user profile of a logon smart card 19. When a logon smart card 19 verifies that a platform 10 is an "extremely trusted" platform 10, it passes user profile information to the platform 10 that includes an option to allow the user to select, from the secure process, a profile modification option. When the user selects the registration process, a special smart card registration process 'wizard' is displayed. This wizard allows the user to add a new auxiliary smart card 20, delete an existing auxiliary smart card 20, and view the detailed information of each auxiliary smart card 20's ID, such as its public key or certificate. In the user profile, each registered smart card has a distinguished number and name given during its registration. 'Wizards' are well known in the art of computer applications, and will not be described in any further detail herein.

In alternative embodiments, the user profile information may be stored in the trusted device 24 or in a remotely located trusted platform 10. Such arrangements would typically require different mechanisms for controlling access by the secure process or platform 10 to the user profile information, but the use of the information once accessed would remain the same.

While the invention has been described with reference to several preferred embodiments, it will be appreciated that various modifications can be made to the parts and methods that comprise the invention without departing from the spirit and scope thereof.

REFERENCES:

[1] ISO/IEC 9798-3, "Information technology – Security techniques – Entity authentication mechanisms; Part 3; Entity authentication using a public key algorithm", International Organization for Standardization, November 1993.

[2] ISO/IEC DIS 11770-3 DRAFT, "Information technology – Security techniques – Key management - Part 3: Mechanisms using asymmetric techniques", International Organization for Standardization, March 1997.

CLAIMS

(HP Ref: 30980059)

1. Computing apparatus comprising:

memory means storing the instructions of a secure process and an authentication process;

processing means arranged to control the operation of the computing apparatus including by executing the secure process and the authentication process as required;

user interface means arranged to receive user input and return to the user information generated by the processing means in response to the user input; and

interface means for receiving a removable primary token and communicating with the token, the token comprising a body supporting:

a token interface for communicating with the interface means;

a token processor; and

token memory storing token data including information for identifying the token,

wherein the processing means is arranged to receive the identity information from the primary token, authenticate the token using the authentication process and, if the token is successfully authenticated, permit a user to interact with the secure process via the user interface means,

and wherein the processing means is arranged to repeatedly authenticate the primary token and cause the computing platform to suspend interaction between the secure process and the user if authentication is not possible as a result of the removal of the primary token.

2. Computing apparatus according to claim 1, arranged to generate information representing the integrity of the computing apparatus and transmit the integrity information to the primary token, wherein the token processor is programmed to verify the integrity of the computing apparatus including by using the integrity information.

3. Computing apparatus according to claim 1 or claim 2, wherein the token data includes auxiliary token information identifying one or more authorised auxiliary tokens.

4. Computing apparatus according to claim 3, arranged to read the auxiliary token information and, in the event the primary token is replaced by a different token, detect whether the different token is an authorised auxiliary token.

5. Computing apparatus according to claim 4, arranged, if the different token is an authorised token, to allow the secure process to interact with the authorised token.

6. Computing apparatus according to claim 5, wherein the authorised token is a cash token and the secure process is arranged to credit or debit the token.

7. Computing apparatus according to claim 5, wherein the authorised token is a crypto token programmed to encrypt, decrypt or sign data, and the secure process is arranged to transmit data to the crypto token to be encrypted, decrypted or signed and receive encrypted, decrypted or signed data from the crypto token.

8. Computing apparatus according to any one of claims 4 to 7, arranged, only if the different token is an authorised auxiliary token, to allow the user to interact with the secure process.

9. Computing apparatus according to any one of claims 4 to 8, further comprising timer means programmed with a timeout period, wherein, in the event the different token is an authorised auxiliary token, the computing apparatus resets the timer and continues operation until the timeout period expires, after which time the computing apparatus suspends any interactions between the secure process and either or both the user and the authorised auxiliary token.

10. Computing apparatus according to claim 9, arranged to recommence said interactions in the event the authorised auxiliary token is replaced by the primary token and the computing apparatus is able to authenticate the primary token.

11. Computing apparatus according to any one of claims 4 to 10, arranged to permit interaction between the secure process and only one authorised auxiliary token after removal of the primary token.

12. Computing apparatus according to any one of claims 4 to 10, arranged to permit interaction between the secure process and more than one authorised auxiliary token after removal of the primary token.

13. Computing apparatus according to any one of the preceding claims, wherein the processing means comprises a main processing unit and a secure processing unit and the memory means comprises main memory and secure memory.

14. Computing apparatus according to claim 13, comprising a trusted device incorporating the secure processing unit and the secure memory, wherein the trusted device is programmed to authenticate the primary token repeatedly.

15. Computing apparatus according to claim 14, wherein the trusted device is arranged to acquire an integrity metric of the computing apparatus, and the primary token is arranged to use the integrity metric on at least one occasion to verify the integrity of the computing apparatus.

16. Computing apparatus according to any one of the preceding claims, wherein the primary token comprises a smart card, and the interface means is configured to receive a smart card.

17. Computing apparatus according to any one of claims 3 to 16, wherein the auxiliary token information is stored in a user profile.

18. A method of controlling computing apparatus to authenticate a user, comprising the steps:

the computing apparatus receiving a primary token of the user, the primary token containing information suitable for authenticating the primary token;

if the token is authentic, permitting the user to interact with one or more secure applications that may be executed by the computing platform;

at intervals, re-authenticating the primary token; and

if it is not possible to re-authenticate the primary token, suspending the interaction between the computing apparatus and the user.

19. A method according to claim 18, further comprising the steps:

the computing apparatus providing integrity metric information to the primary token;

the primary token using the integrity metric information to verify the integrity of the computing apparatus; and

if the primary token is unable to verify the integrity of the computing apparatus, suspending interaction between the computing apparatus and the user.

20. A method according to claim 18 or claim 19, in which the primary token includes information relating to one or more authorised auxiliary tokens, wherein, if the user replaces the primary token with an authorised auxiliary token, the computing apparatus permits interaction between the auxiliary token and the computing apparatus.

21. A method according to claim 20, wherein the computing apparatus interaction with the authorised auxiliary token for a limited period of time.

22. A method according to claim 20 or claim 21, wherein the computing apparatus only permits interaction with one authorised auxiliary token after removal of the primary token.

23. A method according to claim 20 of claim 21, wherein the computing apparatus permits interaction with plural authorised auxiliary tokens after removal of the primary token.

24. A smart card programmed for operation in accordance with any one of claims 18 to 23.

25. Computing apparatus configured for operation in accordance with any one of claims 18 to 23.

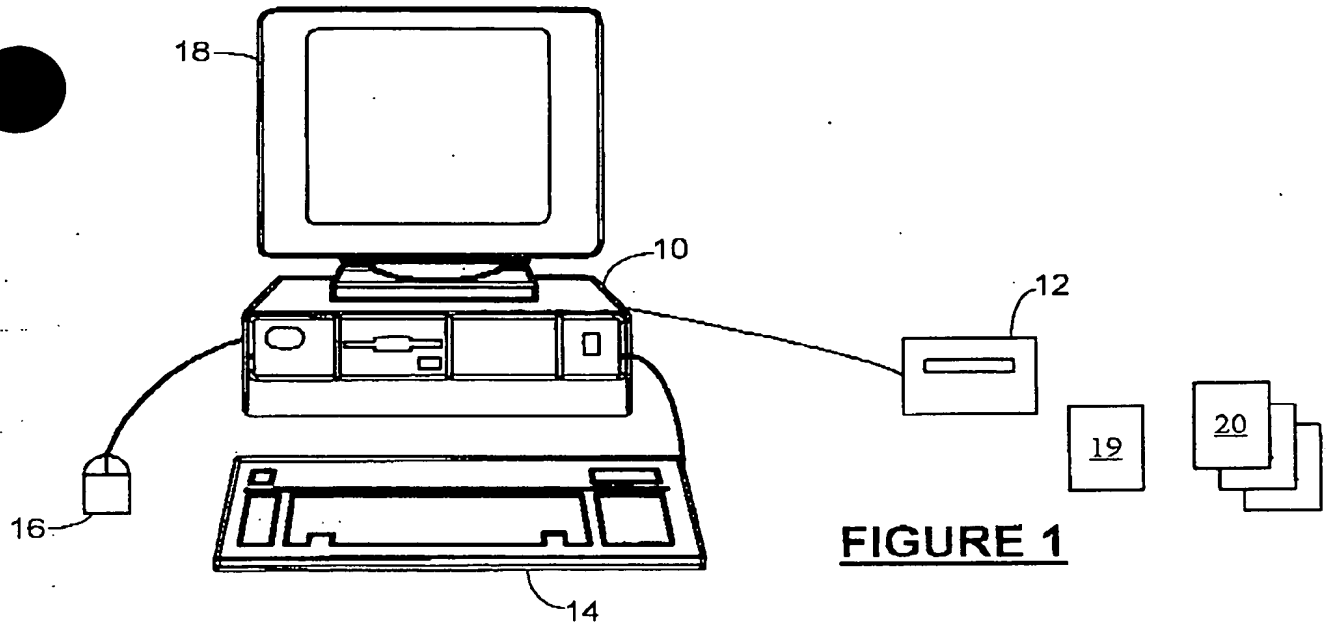

FIGURE 1

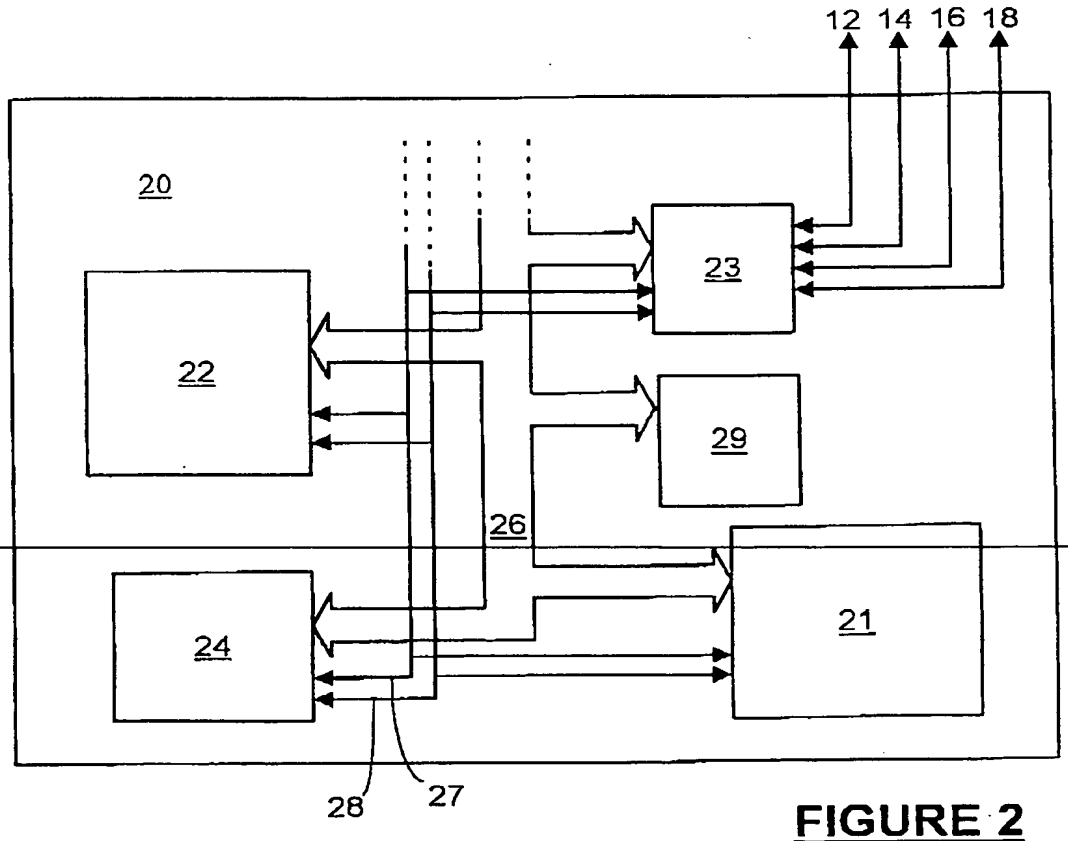

FIGURE 2

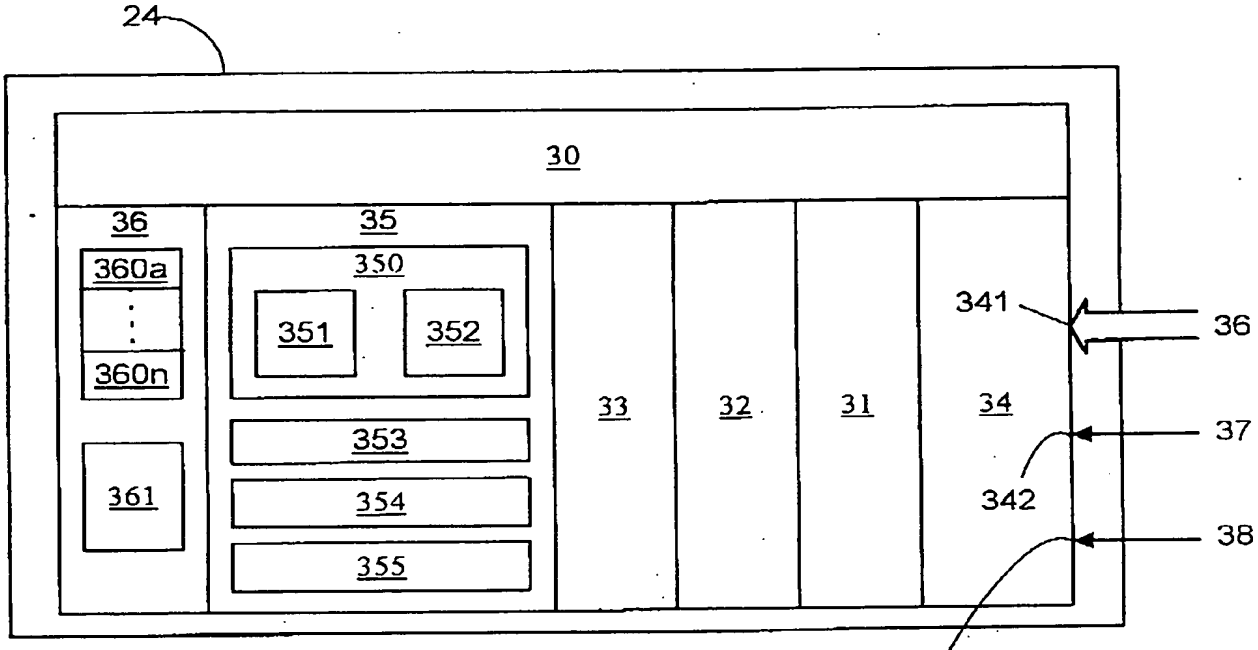

FIGURE 3

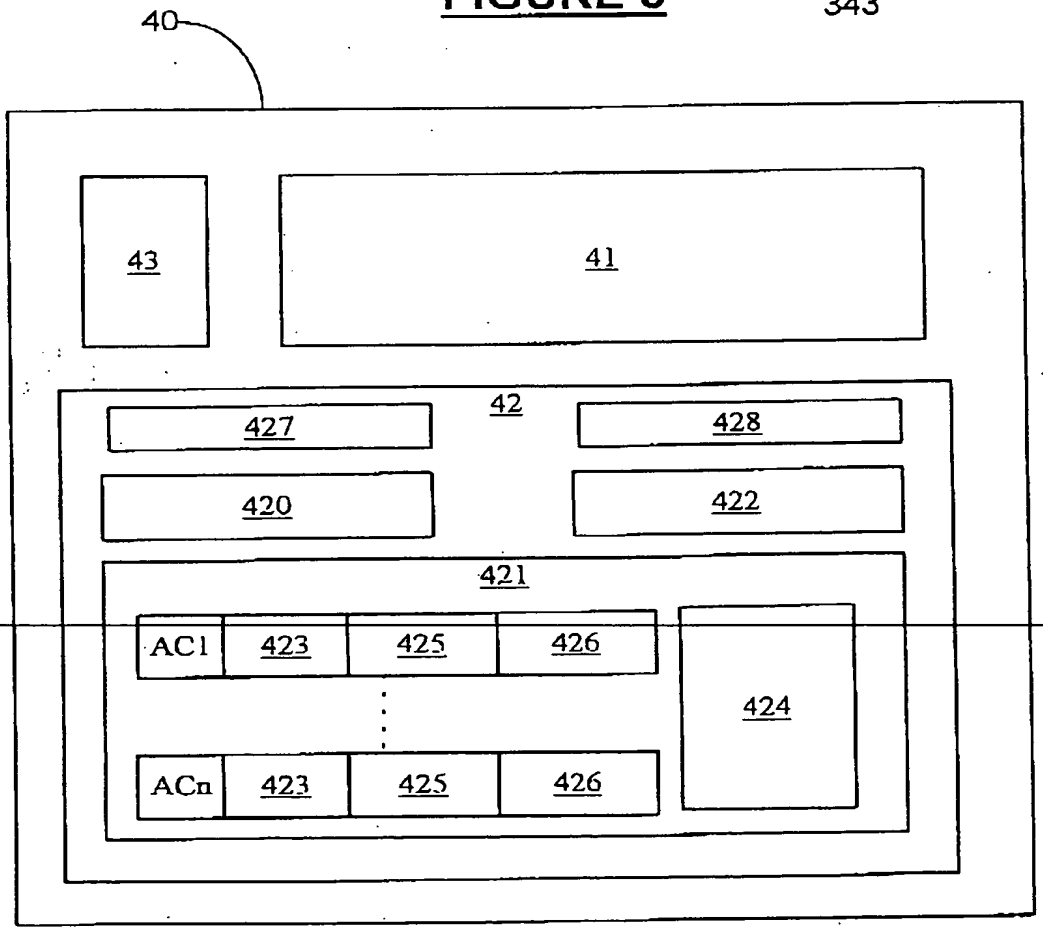

FIGURE 4

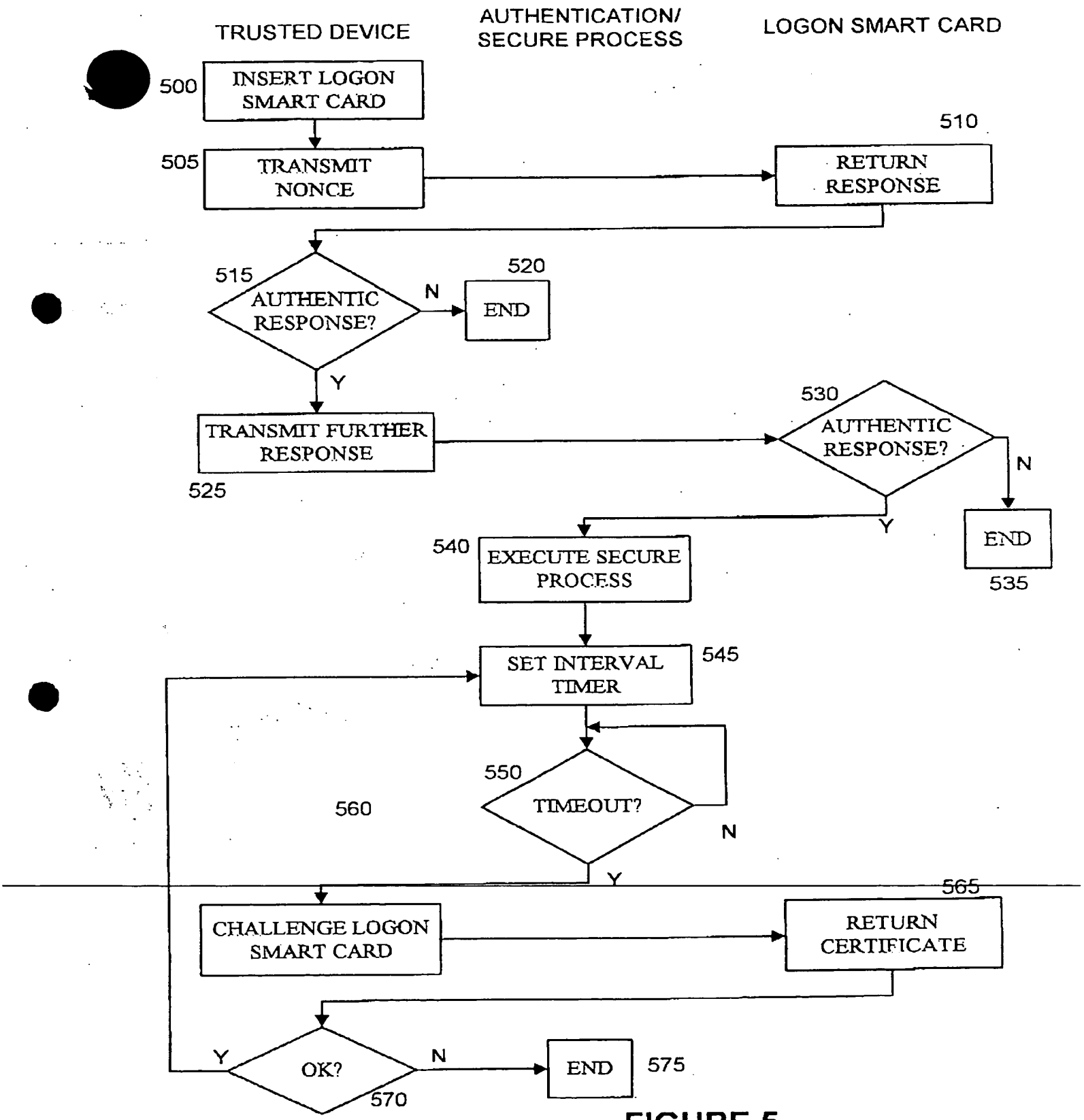
TRUSTED DEVICE
AUTHENTICATION/ SECURE PROCESS
LOGON SMART CARD
500
INSERT LOGON SMART CARD
505
TRANSMIT NONCE
510
RETURN RESPONSE
515
AUTHENTIC RESPONSE?
N
520
END
Y
TRANSMIT FURTHER RESPONSE
525
530
AUTHENTIC RESPONSE?
N
END
535
Y
540
EXECUTE SECURE PROCESS
SET INTERVAL TIMER
545
550
TIMEOUT?
N
560
Y
CHALLENGE LOGON SMART CARD
565
RETURN CERTIFICATE
Y
OK?
N
570
END
575

FIGURE 5

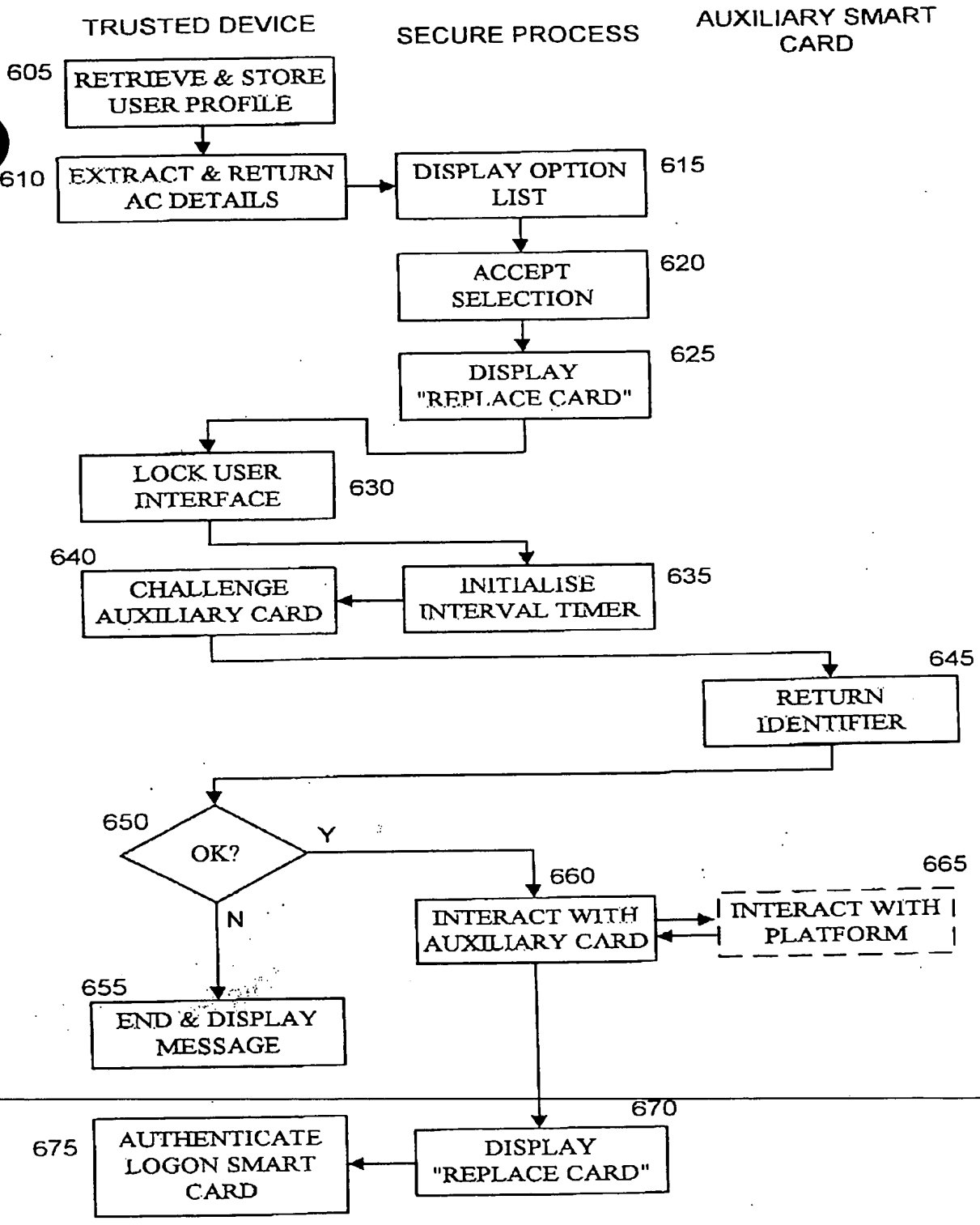
TRUSTED DEVICE
SECURE PROCESS
AUXILIARY SMART CARD
605
RETRIEVE & STORE USER PROFILE
610
EXTRACT & RETURN AC DETAILS
DISPLAY OPTION LIST
615
ACCEPT SELECTION
620
DISPLAY "REPLACE CARD"
625
LOCK USER INTERFACE
630
640
CHALLENGE AUXILIARY CARD
INITIALISE INTERVAL TIMER
635
645
RETURN IDENTIFIER
650
OK?
Y
N
660
INTERACT WITH AUXILIARY CARD
665
INTERACT WITH PLATFORM
655
END & DISPLAY MESSAGE
670
675
AUTHENTICATE LOGON SMART CARD
DISPLAY "REPLACE CARD"

FIGURE 6

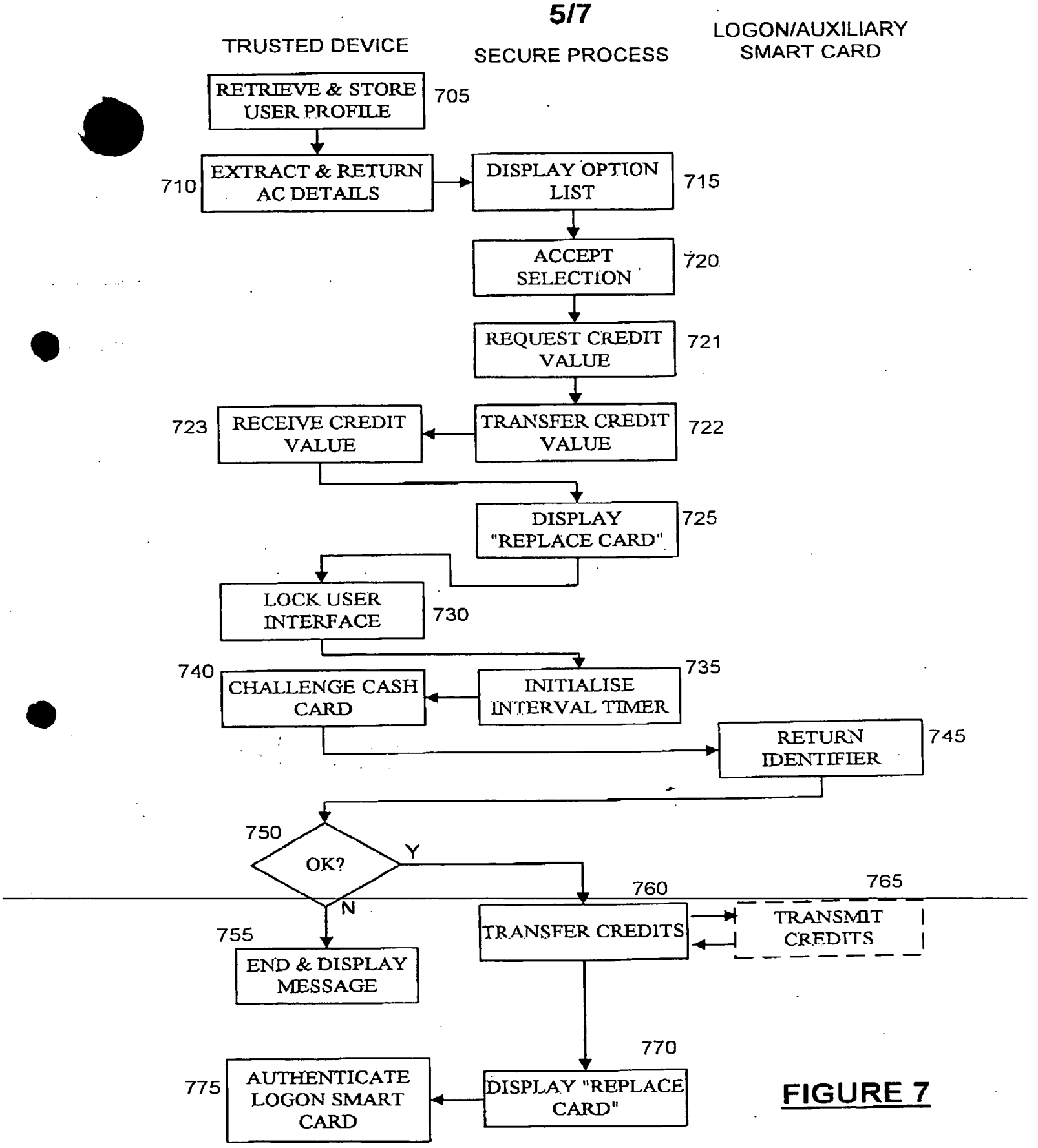
TRUSTED DEVICE
SECURE PROCESS
LOGON/AUXILIARY SMART CARD
RETRIEVE & STORE USER PROFILE
705
EXTRACT & RETURN AC DETAILS
710
DISPLAY OPTION LIST
715
ACCEPT SELECTION
720
REQUEST CREDIT VALUE
721
TRANSFER CREDIT VALUE
722
RECEIVE CREDIT VALUE
723
DISPLAY "REPLACE CARD"
725
LOCK USER INTERFACE
730
INITIALISE INTERVAL TIMER
735
CHALLENGE CASH CARD
740
RETURN IDENTIFIER
745
OK?
750
Y
N
TRANSFER CREDITS
760
TRANSMIT CREDITS
765
END & DISPLAY MESSAGE
755
DISPLAY "REPLACE CARD"
770
AUTHENTICATE LOGON SMART CARD
775

FIGURE 7

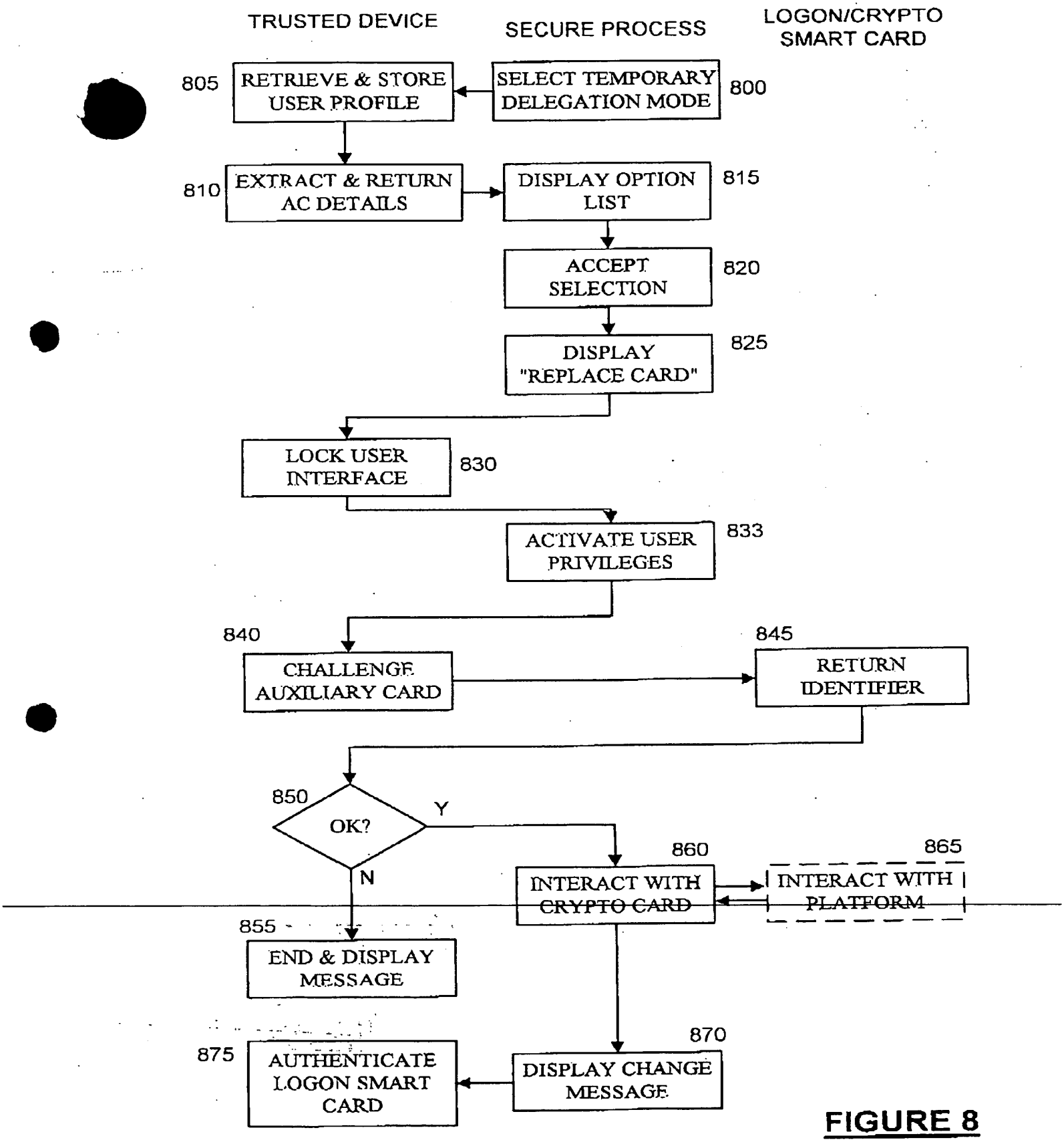
TRUSTED DEVICE
SECURE PROCESS
LOGON/CRYPTO SMART CARD
805
RETRIEVE & STORE USER PROFILE
SELECT TEMPORARY DELEGATION MODE
800
810
EXTRACT & RETURN AC DETAILS
DISPLAY OPTION LIST
815
ACCEPT SELECTION
820
DISPLAY "REPLACE CARD"
825
LOCK USER INTERFACE
830
ACTIVATE USER PRIVILEGES
833
840
CHALLENGE AUXILIARY CARD
845
RETURN IDENTIFIER
850
OK?
Y
N
860
INTERACT WITH CRYPTO CARD
865
INTERACT WITH PLATFORM
855
END & DISPLAY MESSAGE
870
875
AUTHENTICATE LOGON SMART CARD
DISPLAY CHANGE MESSAGE

FIGURE 8

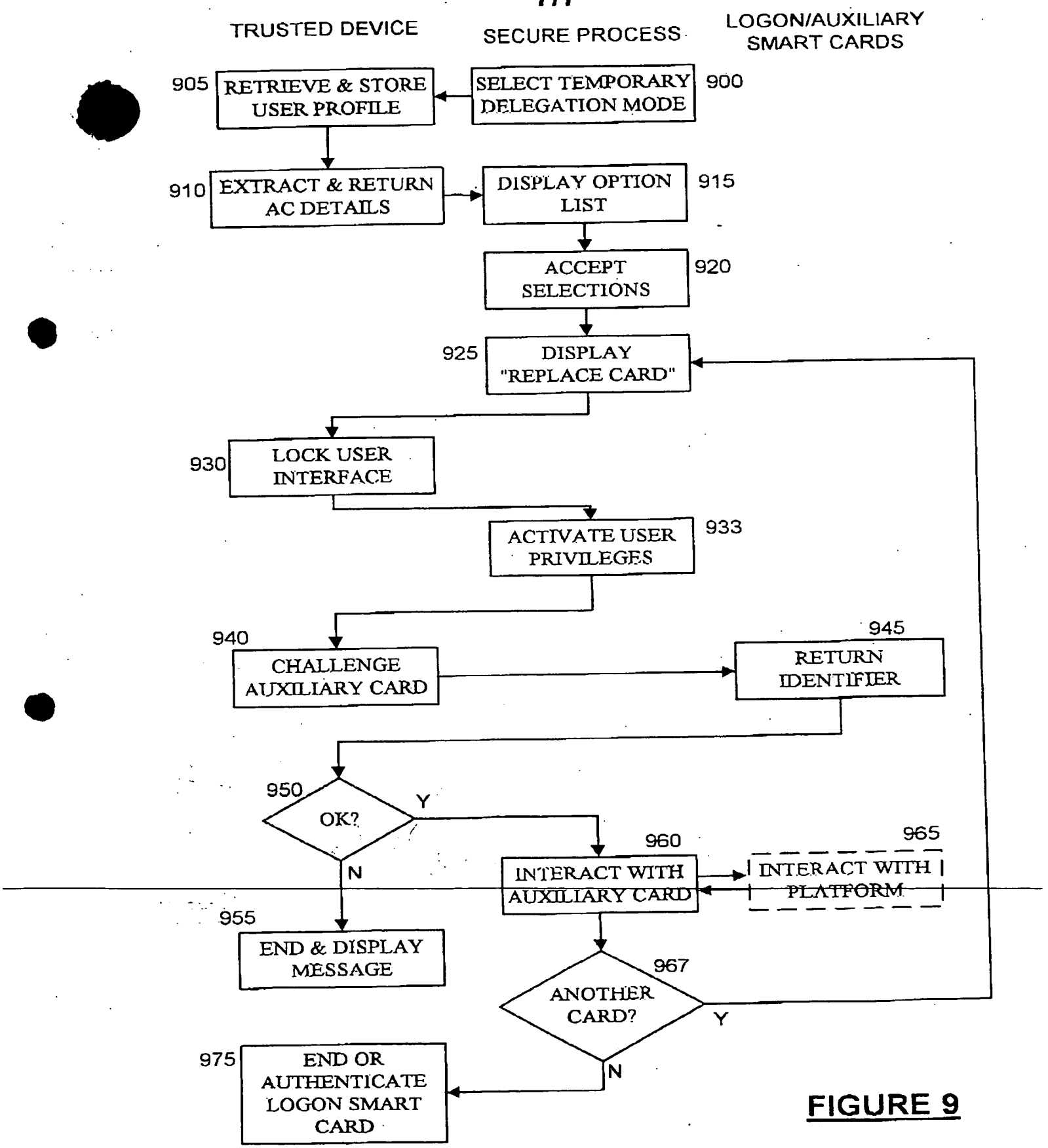
TRUSTED DEVICE
SECURE PROCESS
LOGON/AUXILIARY SMART CARDS
SELECT TEMPORARY DELEGATION MODE
900
905
RETRIEVE & STORE USER PROFILE
910
EXTRACT & RETURN AC DETAILS
DISPLAY OPTION LIST
915
ACCEPT SELECTIONS
920
925
DISPLAY "REPLACE CARD"
930
LOCK USER INTERFACE
ACTIVATE USER PRIVILEGES
933
940
CHALLENGE AUXILIARY CARD
945
RETURN IDENTIFIER
950
OK?
Y
N
960
INTERACT WITH AUXILIARY CARD
965
INTERACT WITH PLATFORM
955
END & DISPLAY MESSAGE
967
ANOTHER CARD?
Y
N
975
END OR AUTHENTICATE LOGON SMART CARD

FIGURE 9